Requested Patent: WO0159686A1

Title: ANTI-FRAUD CHARGE/DATA CARD ;

Abstracted Patent: WO0159686 ;

Publication Date: 2001-08-16 ;

Inventor(s): SHAHAR GALI (IL) ;

Applicant(s): SHAHAR GALI (IL) ;

Application Number: WO2000IL00860 20001226 ;

Priority Number(s): US20000181554P 20000210 ;

IPC Classification: G06K5/00; G06K7/08; G06K7/10; G06K19/00 ;

Equivalents:

AU2216401, CA2400105, EP1279138, JP2003523020T ;

ABSTRACT:

An anti-fraud charge/data card (10) utilizable upon authentication by the card owner is provided. The charge/data card comprises: (a) a first data storage medium (12) being for storing information including stored biometric identification information of the card owner; (b) a second data storage medium (14) capable of being written repeatedly; and (c) a verification assembly (16) including: (i) a power source (18) for powering the verification assembly; (ii) a biometric verification interface for inputting temporary biometric identification information, the temporary biometric information being stored in the second data storage medium; and (iii) a processor (22) for comparing the stored biometric information and the temporary biometric information, such that in the case of a positive match, the processor authorizes use of the charge/data card.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 August 2001 (16.08.2001)

PCT

(10) International Publication Number
WO 01/59686 A1

(51) International Patent Classification[7]: G06K 5/00, 7/08, 7/10, 19/00

(21) International Application Number: PCT/IL00/00860

(22) International Filing Date:
26 December 2000 (26.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/181,554 10 February 2000 (10.02.2000) US

(71) Applicant and
(72) Inventor: SHAHAR, Gali [IL/IL]; 42a Nordau Street, 46 582 Herzlia (IL).

(74) Agent: G. E. EHRLICH (1995) LTD.; Bezalel Street 28, 52 521 Ramat Gan (IL).

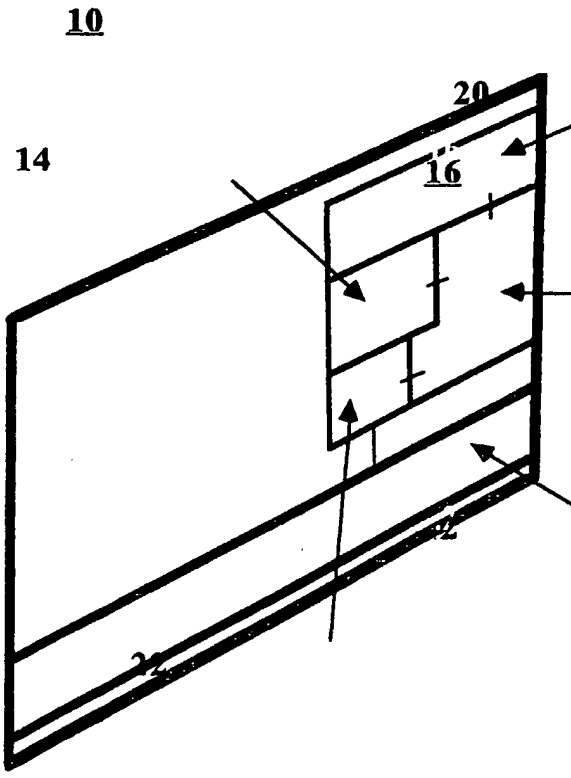
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ANTI-FRAUD CHARGE/DATA CARD



(57) Abstract: An anti-fraud charge/data card (10) utilizable upon authentication by the card owner is provided. The charge/data card comprises: (a) a first data storage medium (12) being for storing information including stored biometric identification information of the card owner; (b) a second data storage medium (14) capable of being written repeatedly; and (c) a verification assembly (16) including: (i) a power source (18) for powering the verification assembly; (ii) a biometric verification interface for inputting temporary biometric identification information, the temporary biometric information being stored in the second data storage medium; and (iii) a processor (22) for comparing the stored biometric information and the temporary biometric information, such that in the case of a positive match, the processor authorizes use of the charge/data card.

WO 01/59686 A1

ANTI-FRAUD CHARGE/DATA CARD

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to an anti-fraud charge/data card and, more particularly, to an anti-fraud charge/data card which includes a verification assembly which is capable of comparing biometric identification information stored in the card with biometric identification information acquired from the card holder to thereby grant use only to a legitimate card holder.

Charge/data cards carrying magnetic stripes or other means of interfacing with a card reader are widely used as credit cards, debit cards, automatic teller machine (ATM) cards, telephone payment cards, authentication (e.g., for access authorization) cards, etc.

Typically, magnetic stripe cards hold approximately 200 alphanumeric characters, which is equivalent to 200 bytes of data in computer language. The magnetic stripe is erasable and is read and written by a wide variety of commercial devices. In addition, smart cards which contain chips and memory and which use a variety of port configurations and powering sources are also well known in the art.

A variety of methods are used to enhance the security of such cards so as to discourage counterfeiting and/or fraudulent use.

For example, in magnetic cards, holograms are affixed to the cards to make card counterfeiting more difficult. To discourage fraudulent use, a color photograph of the registered card owner's face is affixed to the card and serves for confirmation that the possessor of the card is the rightful owner. Personal identification numbers (PIN) are memorized by the card owner and entered into terminals such as bank ATM terminals to prove card ownership prior to cash payments to the card possessor.

In spite of all the anti-fraud methods currently used, fraudulent use of magnetic stripe cards results in losses estimated at from many hundreds of millions of dollars to billions of dollars annually. The fraudulent methods involve a variety of techniques. Magnetic stripe cards are stolen. Lost cards are found and used. Cards are counterfeited. A person may apply for and have cards issued in the names of unsuspecting credit-worthy individuals. PIN numbers may be obtained by observing an ATM user entering his number or finding a PIN number noted in a lost or stolen wallet. Internet card number theft has also increased dramatically in recent years.

As such, numerous methods for preventing counterfeit or fraudulent use of cards have been described in the prior art.

For example, U.S. Pat. No. 4,614,861 to Pavlov et al. describes a unitary, self-contained card which does not require interaction with a fixed terminal device to prevent monitoring of confidential information contained within the card. The unitary, self-contained card according to this patent has the ability to verify a personal identification number which is entered directly into the card by way of a keyboard without the use of an outside terminal. Once a code is verified, a transaction identification code is produced which varies for each transactional use of the card and which can later be verified to determine the validity of the transaction. The card is capable of storing issue and expiration dates, credit limit balances and other card transactional data. The card can be used in conjunction with a validation system with provisions for verifying information recorded on the magnetic indicia of the card. The card can also be used with peripheral devices which function to verify the validity of the transaction from the transaction identification code.

Although such a card design decreases the chances of fraudulent use or counterfeiting, the use of a code or codes for activation still enables fraudulent use, since any person gaining access to the code can activate and therefore use the card.

To solve such problems, Drexler et al. describes in U.S. Pat. No. 5,457,747 a system for deterring fraudulent use of wallet-size cards in local benefit dispensing terminals. The system according to Drexler et al. has a permanent data storage medium and a temporary data storage medium disposed on each card. A first card writing device has means for acquiring biometric information from a person and for writing a template of that information on the permanent storage medium. A verification terminal has similar means for acquiring biometric information from a possessor of the card, and also has a means for reading the biometric information from the permanent storage medium of the card. Upon inputting biometric information from both the card and the possessor of the card, the verification terminal compares the information, and, if they match, writes data allowing limited benefits on the temporary data storage medium of the card. This data can be read by a plurality of existing benefit dispensers at other locations, such as automated teller machines, which can then dispense benefits authorized by the data. The

limitation on benefits and the required repeated verification enhances security of the cards and the benefit dispensing system.

Since such a card system uses biometric information for card ownership verification, the chances of fraudulent use or counterfeiting are minimized. However, activation of this card requires the use of an activation terminal which greatly complicates the use of this card

There is thus a widely recognized need for, and it would be highly advantageous to have, a charge/data card with a self contained authentication assembly which is devoid of the above limitation.

SUMMARY OF THE INVENTION

Thus, according to one aspect of the present invention there is provided a charge/data card utilizable upon authentication by the card owner, the charge/data card comprising (a) a first data storage medium being for storing information including stored biometric identification information of the card owner; (b) a second data storage medium capable of being written repeatedly; and (c) a verification assembly including (i) a power source for powering the verification assembly; (ii) a biometric verification interface for inputting temporary biometric identification information, the temporary biometric information being stored in the second data storage medium; and (iii) a processor for comparing the stored biometric information and the temporary biometric information, such that in the case of a positive match, the processor authorizes use of the charge/data card.

According to another aspect of the present invention there is provided a method for authorizing card use to a charge/data card holder, the method comprising the step of (a) acquiring biometric identification information from the charge/data card holder and storing the biometric identification information in a first storage medium of the charge/data card; (b) comparing the stored biometric identification information with subsequently acquired biometric identification information acquired via a biometric verification interface included in or on the charge/data card; and (c) if the stored biometric information and the subsequently acquired biometric information positively match, authorizing use of the charge/data card.

According to further features in preferred embodiments of the invention described below, step (c) of the above method is effected by a processor included in the charge/data card.

According to still further features in the described preferred embodiments the stored biometric identification information is inputted into the charge/data card via the biometric verification interface.

According to still further features in the described preferred embodiments the processor authorizes use of the charge/data card for a limited time period.

According to still further features in the described preferred embodiments the processor authorizes use of the charge/data card only in limited types of transaction.

According to still further features in the described preferred embodiments the processor authorizes use of the charge/data card up to a limited charge amount.

According to still further features in the described preferred embodiments the first and the second storage media are each individually selected from the group consisting of a magnetic stripe, an optical recording and a memory chip.

According to still further features in the described preferred embodiments the stored and the temporary biometric identification information are each selected from the group consisting of a fingerprint, a retina scan, a voice print and a signature.

According to still further features in the described preferred embodiments the first and the second storage media are a single storage medium.

The present invention successfully addresses the shortcomings of the presently known configurations by providing an anti-fraud charge/data card which includes a verification assembly for granting use only to a legitimate owner of the card.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is herein described, by way of example only, with reference to the accompanying drawings. With specific reference now to the drawings in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental

understanding of the invention, the description taken with the drawings making apparent to those skilled in the art how the several forms of the invention may be embodied in practice.

In the drawings:

FIG. 1 is a perspective view of the anti-fraud charge/data card of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is of an anti fraud charge/data card which includes a verification system which can be used to authorize use of the card only to a legitimate card holder. Specifically, the present invention can be used to enable a legitimate charge/data card holder limited or unlimited use of the charge/data card by acquiring biometric information from the charge/data card holder and comparing this biometric identification information with a similar type of biometric identification information permanently stored within the card.

The principles and operation of the present invention may be better understood with reference to the drawing and accompanying descriptions.

Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and the arrangement of the components set forth in the following description or illustrated in the drawing. The invention is capable of other embodiments or of being practiced or carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein is for the purpose of description and should not be regarded as limiting.

As used herein the phrase "charge/data card" refers to any card capable of performing credit transaction or payment, such as but not limited to, credit cards, debit cards, membership cards and any personal identification/authentication card which entitles the holder to benefits or access. As such a charge/data card may include any element for interfacing with a card reader, such as, but not limited to, magnetic or optic stripes, and/or any other data ports. Preferably the charge/data card of the present invention is similar in shape, size and thickness to a standard wallet size credit card.

As used herein the phrase "biometric identification information" includes individual characteristics such as a fingerprint or fingerprints, a

voice-print, a retinal scan or a signature which are unique to the individual from which the information was acquired.

Referring now to the drawing, Figure 1 illustrates the anti-fraud charge/data card of the present invention, which is referred to hereinbelow as card **10**.

Card **10** includes a first data storage medium **12** which serves for permanently storing information including biometric identification information of the card owner which is preferably written in a compressed or a template form. Such information can be inputted into the card by the card supplier, or alternatively by the card holder using the biometric verification interface described hereinbelow.

Storage medium **12** can also serve for storing additional information of the card holder such as bank account number, and the like which can be accessed by, for example, an interfacing card reader terminal, when the card is in use. Storage medium **12** may be an optic or a magnetic stripe which can be written by a magnetic or a laser recording device, and read by the same or another device in order to retrieve the stored information. Storage medium **12** may be a non-erasable memory such as a semiconductor chip which is recorded in a programmable read only memory (PROM). Any other medium which can store moderate to large amount of information in a thin area which can be written upon and later retrieved can be used as the storage medium **12**. It will be appreciated that storage medium **12** can be written or read directly, such as the case with a magnetic or optic stripe, or alternatively, and in the case of, for example, a semiconductor chip, storage medium **12** can communicate with data ports provided in or on card **10** so as to enable a suitable card reader provided with similar ports to read information from and/or write information into, data storage medium **12**.

Storage medium **12** can be divided into various storage regions for separately storing the biometric identification information and the other personal information described above, such that a card reader terminal, for example, can only access the stored personal information and not the biometric identification information, an example of such a storage medium suitable for use with charge/data cards is described in U.S. Pat. No. 4,683,371 which is incorporated herein by reference.

Card **10** further includes a second data storage medium **14** which is capable of being written repeatedly and which serves for temporarily

storing biometric information acquired from the card holder as is further detailed hereinunder.

According to a preferred embodiment of the present invention storage medium **14** is preferably a read write capable storage device such as, but not limited to, a random access memory (RAM) chip.

Card **10** of the present invention further includes a verification assembly **16** which serves to verify the identity of the card holder.

Verification assembly **16** includes a power source **18** for powering assembly **16**. Such a power source is preferably a miniature battery of a size and thickness suitable for implementation into card **10**. An example to a suitable power source **18** is described in U.S. Pat. No. 5,652,043, which teaches a thin layer flexible battery. the teachings of U.S. Pat. No. 5,652,043 are incorporated herein by reference.

Verification assembly **16** further includes a biometric verification interface **20** which is in communication with data storage medium **14**. Interface **20** enables a card holder to record biometric identification information into data storage medium **14**, in which, the recorded information is stored, preferably temporarily. Interface **20** can include any device capable of recording biometric identification information which can be devised thin enough so as to be integrated into card **10**.

For example, interface **20** can include a miniature and flat microphone, such as, for example, those microphones used in hearing aid devices, or that microphone described in U.S. Pat. No. 5,490,220, which is incorporated herein by reference, which can record a voice-print to be stored in data storage medium **14**. Alternatively interface **20** can include a miniature camera for recording a retinal image. Such a camera is preferably based on planar optics technology and compatible CCD devices so as to fit the thin and planar nature of card **10**. Interface **20** can still alternatively include a miniaturized touch screen, which is planar by nature, for recording an electronic signature or a finger print, the use of digitally encoded finger print information for biometric identification is described in, for example, U.S. Pat. No. 5,053,608 which is incorporated herein by reference. Further details relating to biometric features analysis, including hand and face geometry can be found in Biometricgroup.com and biometric.ca, the data contained in both of which is incorporated herein by reference.

Assembly **16** further includes a processor **22** which serves to process the stored and temporarily acquired biometric identification

information. Processor **22** is in communication with data storage media **12** and **14** such that biometric information stored thereby is made available to processor **22**.

Processor **22** serves for comparing the biometric identification information stored in data storage medium **12** with the biometric identification information acquired from the card holder and temporarily stored in data storage medium **14**. It will be appreciated that in order to effect this comparison, processor **22** must be provided with a suitable software program which is preferably stored in a memory chip of processor **22**. Such a software program would enable processor **22** to compare the biometric identification information stored in data storage media **12** and **14** for matching characteristic parameters thereof. For example, if the biometric information is a voice print, the frequency, pitch and/or waveform of the voice print can be compared by processor **22**. Techniques of voice verification have been extensively described in, for example, U.S. Pat. Nos. 5,502,759; 5,499,288; 5,414,755; 5,365,574; 5,297,194; 5,216,720; 5,142,565; 5,127,043; 5,054,083; 5,023,901; 4,468,204 and 4,100,370, all of which are incorporated by reference as if fully set forth herein. These patents describe numerous methods for voice verification. Similarly, software capable of comparing signatures (U.S. Pat. Nos. 5,892,824; and 5,838,815), eye-scans (U.S. Pat. No. 5,973,731) and fingerprints (U.S. Pat. No. 5,999,637) are well known in the art. U.S. Pat. Nos. 5,892,824; 5,838,815; 5,973,731; and 5,999,637 are incorporated herein by reference.

If the biometric identification information stored in data storage medium **12** matches that acquired from the card holder the identity of the card holder has been verified, and processor **22** writes an authorization code on data storage medium **14** which activates charge/data card **10**. It will be appreciated that this activation can be effected by one of several methods. For example, if card **10** includes a magnetic or an optic stripe for interfacing with a card reader, then the authorization code can allow card readers access to the personal information included in this stripe. Alternatively if the card includes data ports typical of smart cards, then such an authorization code activates ports and allows access to personal information.

In any case, the authorization code may allow use that is limited in amount, limited in time, limited in form, limited in geography, limited in the type of interfacing readers, for example allowing a credit card to

interface with ATM machines but not credit card readers, or have a combination of these limits. For example, an activation code may only allow benefits to be dispensed from a local benefit dispenser for a day, a week or a month from a starting time. On the other hand, the activation code may allow only one hundred dollars to be dispensed, or may allow up to that amount to be dispensed for one month after the time of verification. This limit on the benefits which can be obtained from card **10** before re-verification creates a ceiling on the benefits that can be fraudulently obtained. In addition, card **10** may be designed to serve several users, such as members of a family, in a fashion similar to that described above for a single user, each of the users being identified by comparison between stored and temporary biometric information. Different limitations and restrictions may apply to different users of a multiusers card **10**.

Thus, the present invention describes an anti-fraud charge/data card which contains a verification assembly for verifying the identity of the card holder.

It will be appreciated that a charge/data card which includes a verification assembly as described by the present invention is advantageous to both the user and the service or card provider, since such a card does not require a separate stationary or mobile verification assembly, which entails added costs to the card provider and/or holder and which greatly complicates card activation and as such severely detracts from the cards' utility.

Although the invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, it is intended to embrace all such alternatives, modifications and variations that fall within the spirit and broad scope of the appended claims. All publications cited herein are incorporated by reference in their entirety. Citation or identification of any reference in this application shall not be construed as an admission that such reference is available as prior art to the present invention.

WHAT IS CLAIMED IS:

1. A charge/data card utilizable upon authentication by the card owner, the charge/data card comprising,

(a) a first data storage medium being for storing information including stored biometric identification information of the card owner;

(b) a second data storage medium capable of being written repeatedly; and

(c) a verification assembly including:

(i) a power source for powering said verification assembly;

(ii) a biometric verification interface for inputting temporary biometric identification information, said temporary biometric information being stored in said second data storage medium; and

(iii) a processor for comparing said stored biometric information and said temporary biometric information, such that in the case of a positive match, said processor authorizes use of the charge/data card.

2. The charge/data card of claim 1, wherein said stored biometric identification information is inputted into the charge/data card via said biometric verification interface.

3. The charge/data card of claim 1, wherein said processor authorizes use of the charge/data card for a limited time period.

4. The charge/data card of claim 1, wherein said processor authorizes use of the charge/data card only in limited types of transaction.

5. The charge/data card of claim 1, wherein said processor authorizes use of the charge/data card up to a limited charge amount.

6. The charge/data card of claim 1, wherein said first and said second storage media are each individually selected from the group consisting of a magnetic stripe, an optical recording and a memory chip.

7. The charge/data card of claim 1, wherein said stored and said temporary biometric identification information are each selected from the group consisting of a fingerprint, a retina scan, a voice print and a signature.

8. The charge/data card of claim 1, wherein said first and said second storage media are a single storage medium.

9. A method for authorizing card use to a charge/data card holder, the method comprising the step of:

(a) acquiring biometric identification information from the charge/data card holder and storing said biometric identification information in a first storage medium of the charge/data card;

(b) comparing said stored biometric identification information with subsequently acquired biometric identification information acquired via a biometric verification interface included in or on the charge/data card; and

(c) if said stored biometric information and said subsequently acquired biometric information positively match, authorizing use of the charge/data card.

10. The method of claim 9, wherein said stored biometric identification information is acquired by said biometric verification interface.

11. The method of claim 9, wherein step (c) is effected by a processor included in the charge/data card.

12. The method of claim 11, wherein said processor authorizes use of the charge/data card for a limited time period.

13. The method of claim 11, wherein said processor authorizes use of the charge/data card only in limited types of transaction.

14. The method of claim 11, wherein said processor authorizes use of the charge/data card up to a limited charge amount.

15. The method of claim 9, wherein said subsequently acquired biometric identification information is temporarily stored in a second storage medium.

16. The method of claim 15, wherein said first and said second storage media are each individually selected from the group consisting of a magnetic stripe, an optical recording and a memory chip.

17. The method of claim 9, wherein said stored and said subsequently acquired biometric identification information are each selected from the group consisting of a fingerprint, a retina scan, a voice print and a signature.

18. The method of claim 15, wherein said first and said second storage media are a single storage medium.

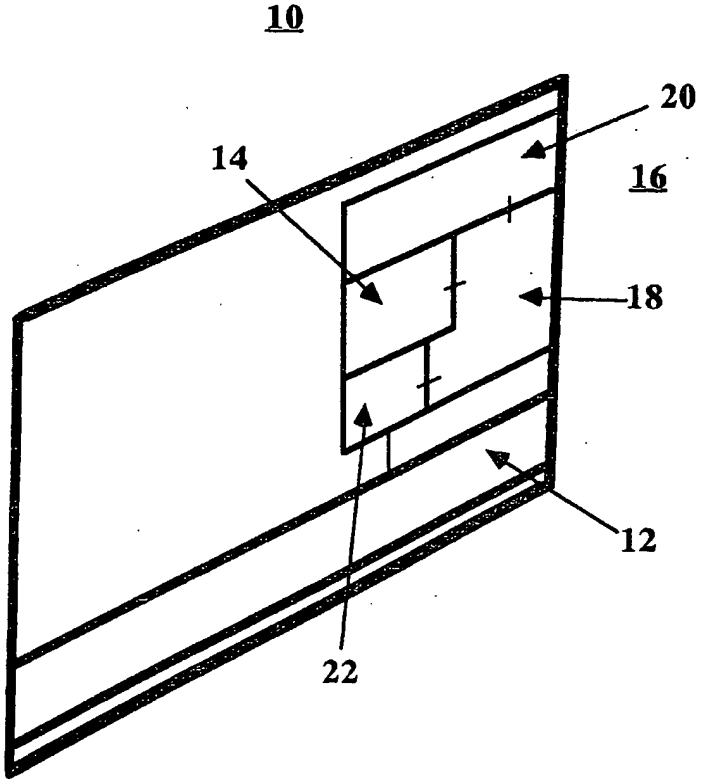


FIG. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00860

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06K 5/00, 7/08, 7/10, 19/00
US CL :235/380, 382, 449, 454, 487; 902/25
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 235/380, 382, 449, 454, 487; 902/25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

NONE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,457,747 A (DREXLER et al) 10 October 1995 (10.10.1995), abstract, figs .1, 3 and col. 3, line 51 - col. 4, line 59.	1, 2, 6-10, 15-18 --- 3-5, 11-14
X	US 4,752,676 A (LEONARD et al) 21 June 1988 (21.06.1988), figs. 1, 4; col. 2, line 60 - col. 3, line 9; and claims 1-3.	1-3, 7, 9, 10, 15-18
X --- Y	US 5,473,144 A (MATHURIN, JR.) 05 December 1995 (05.12.1995), figs. 1, 5, 6; col. 1, line 4 - col. 5, line 67; col. 14, lines 6-23; and col. 15, lines 8-16.	1, 2, 6-10, 15-18 --- 3-5, 11-14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 07 APRIL 2001	Date of mailing of the international search report 01 MAY 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LARRY D TAYLOR Telephone No. (703) 306-5867

Form PCT/ISA/210 (second sheet) (July 1998)★